

## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
1 April 2004 (01.04.2004)

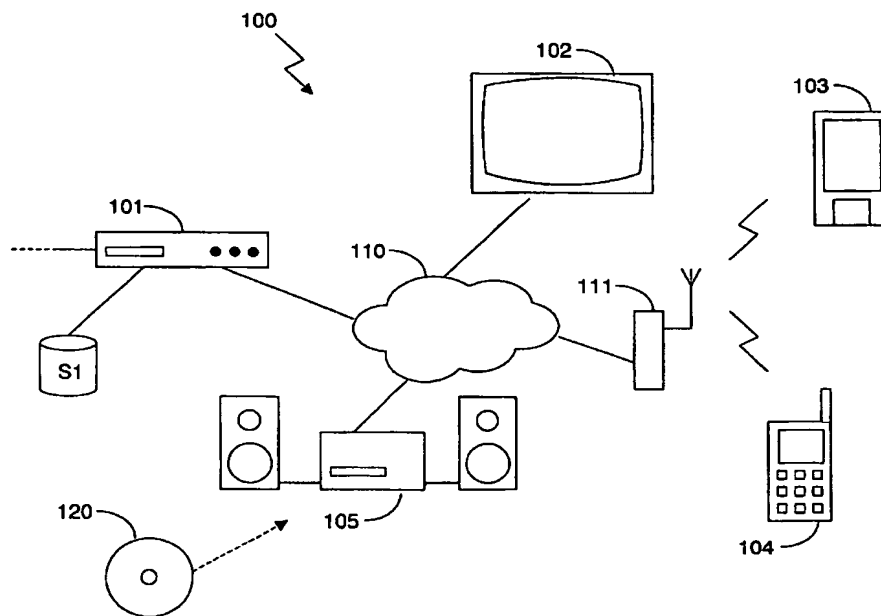
PCT

(10) International Publication Number  
**WO 2004/028075 A1**

- (51) International Patent Classification<sup>7</sup>: **H04L 9/30**
- (21) International Application Number:  
PCT/IB2003/003641
- (22) International Filing Date: 11 August 2003 (11.08.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
02078952.5 20 September 2002 (20.09.2002) EP
- (71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **TUYLS, Pim, T.** [BE/BE]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DIJK, Marten, E.** [NL/US]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **SCHOENMAKERS, Berry** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).
- (74) Agent: **GROENENDAAL, Antonius, W., M.**; Philips Intellectual Property & Standards, Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:  
— with international search report

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR GENERATING A COMMON SECRET KEY



(57) Abstract: A method for generating a common secret data item between a first user facility and a second user facility does so through by each user facility executing mutually symmetric operations on respective complementary data items that are based on respectively unique quantities and that are at least in part secret. An outcome of the operations is used in both said user facilities as said common secret data item. In particular, the method is based on defining the complementary data belonging to a GAP Diffie-Hellmann Problem that is defined in an Abelian Variety. More in particular, the Abelian Variety has a dimension one through being an elliptic curve.